# FAA National Software Conference, May 2002
# Software Service History Research Results

## Software Service History Research Brief-Out

**Ferrell and Associates Consulting, Inc.**

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 1

## Outline

- Research Effort
- Handbook
- Report
- Research Conclusions
- Follow-On Activities
- Conclusion

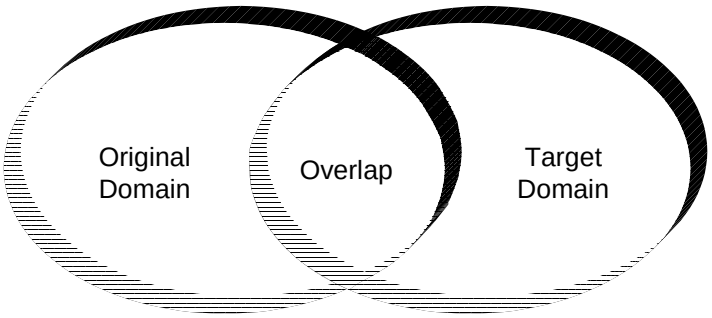
Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 2

Tom & Uma Ferrell

# FAA National Software Conference, May 2002
# Software Service History Research Results

## Domain Intersection




"**Product Service History** – A contiguous period of time during which the software is operated within a known environment, and during which successive failures are recorded."

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 3

## Service History And DO-178B

- Service History is one of the alternate methods
- Acceptability for certification credit is dependent on:
  - Configuration Management of the Software
  - Effectiveness of Problem Reporting
  - Stability and Maturity of Software
  - Relevance of Product Service History Environment
  - Actual Error Rates
  - Impact of Modifications

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 4

## FAA's Call For Research

Although Service History seems to be a fairly straightforward technique, in practice, such use has proved extremely problematic because of the following:

- Difficulty in proving relevance of environment
- Data Consistency from Various "Users"
- Effectiveness of problem reporting
- Stability/Maturity of software
- What is the minimum "duration" of data at different criticality levels
- How to compute "error rates"

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 5

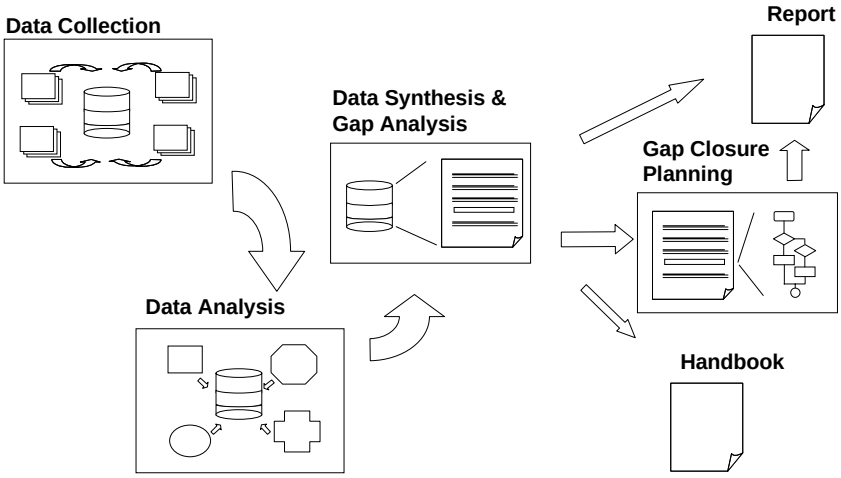
## Research Effort Overview

- Survey existing research and dialogues on the subject of Product Service History (PSH)
- Perform research to include:
  - Synthesis of existing material from various safety-critical industries into a comprehensive handbook
  - Performance of a gap analysis of existing material
  - Solicit feedback from the industry as needed
  - Preparation of a final report for the FAA as an accomplishment summary for the effort
- Effort to include periodic reporting and briefings to the FAA

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 6

## Overall Process




Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 7

## The Questions Taxonomy

- In approaching the research effort, it became apparent that we needed a way to group like issues together.
- We accomplished this by dissecting the PSH definition into four components:
  - Problem Reporting – All issues concerned with problem report contents and problem reporting mechanization
  - Environment – Constrained to those elements relating to the actual computing environment
  - Operation – Second part of 'environment' focused on items outside of the computing environment, nominally operating modes, interaction with users, and procedures
  - Time – All issues concerned with the representation of time as it relates to a service history argument

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 8

## Handbook Outline

- Introduction
- DO-178 Framework
  - The definition
  - **Analysis of Product Service History in DO-178B**
  - Relationship with Previously Developed Software
  - Product Service History Vs. Software Reliability
- The Elements of Product Service History
  - Questions of Problem Reporting
  - Questions of Operation
  - Questions of Environment
  - Questions of Time
- Adequacy of the Development Process
- Establishment of "Equivalent Safety"
- Summary
- Bibliography
- **Appendix A: Evaluation Worksheets**

**DOT/FAA/AR-01/116**

**Software Service History Handbook**

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 9

## Analysis of PSH Guidance in DO-178B

- Table 1 of the Handbook provides a detailed review and analysis of the eleven guidance statements for the use of product service history found in DO-178B, section 12.3.5
- This table is designed to help you understand the underlying rationale behind each of the guidance statements by providing:
  - A set of observations on what is being discussed and where some of the pitfalls may be in satisfying that guidance statement
  - An initial round of questions to ask regarding the available data
  - A clear linkage back to the elements of the definition of PSH through the Questions metaphor used throughout the Handbook
- Use Table 1 to understand "WHY" each guidance statement exists

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 10

## Table 1 Excerpt

| DO-178B Section 12.3.5 Reference | Observations on DO-178B Section 12.3.5 | Software Service History Questions | Questions Category |
|---|---|---|---|
| a. The applicant should show that the software and associated evidence used to comply with system safety objectives have been under configuration management throughout the product service history | If this evidence for safety objectives is missing or non-compliant, there is no workaround.<br><br>The service history data that is associated with software that is not configuration controlled should not be used as evidence since there is no confidence in the data or software. There is no basis for computing error rates. | • Are the software versions tracked during the history duration?<br>• Are problem reports tracked with respect to particular versions of the software?<br>• Are problem reports associated with the solutions/patches and an analysis of change impact?<br>• Is revision/change history maintained for different versions of the software?<br>• Have change impact analyses been performed for changes? | Question of Problem Reporting |

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 11

## Worksheets Overview

- Appendix A contains four worksheets, one for each area of questions relevant to evaluating PSH data.
- The majority of worksheet items relate directly to a section 12.3.5 item.
- A small number of items derived from best practices from other industry sectors have been included only where these practices directly support DO-178B guidance.
- The intent is that these worksheets would be used in the preparation of an alternates means of compliance argument.
- There is NO requirement from the FAA that you must use these – they are simply an aid to you!
- The worksheets should not be considered static – you may need to tailor them for a particular project.

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 12

## Sample Worksheet Excerpt

| # | DO-178B Reference | Question | Response | Issues |
|---|---|---|---|---|
| 1. | 12.3.5 j(2) | What is the definition of service period? | | |
| 2. | 12.3.5 j(2) | Is the service period defined appropriate to the nature of software in question? | | |
| 3. | 12.3.5 j(2) | What is the Definition of normal operation time? | | |
| 4. | 12.3.5 j(2) | Does normal operation time used in the service period include normal and abnormal operating conditions? | | |
| 5. | Glossary | Can contiguous operation time be derived from the service history data? | | |
| 6. | OIS | Is the “applicable service” portion extractable from the total service history data? | | |

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
Slide 13

## Report Outline

- Introduction
- DO-178 Framework
  - The definition
  - Analysis of Product Service History in DO-178B
  - Relationship with Previously Developed Software
  - Product Service History Vs. Software Reliability
- The Elements of Product Service History
  - Questions of Problem Reporting
  - Questions of Operation
  - Questions of Environment
  - Questions of Time
- Adequacy of the Development Process
- Establishment of “Equivalent Safety”
- Research Summary
- Conclusion
- Appendix A: Data Collection and Synthesis
- Appendix B: Literature Search

**DOT/FAA/AR-01/125**

**Software Service History Report**

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.
Slide 14

## Report Overview

- The Report includes the contents of the Handbook and the additional items noted below .
  - The FAA requested that gaps in existing guidance as it relates to service history be identified.
  - These gaps, along with suggested approaches for addressing them are documented for each of the major areas of the PSH definition: problem reporting, time, operation, and environment.
  - The Report also contains the complete results of the literature search, interviews, and selected notes from the research analysis.
- The Report was written primarily for the FAA. Those elements most useful for industry were extracted to the Handbook for ease of use.



## Research Conclusions

- Worksheets- lists of general considerations for evaluating service history.
- Worksheets may be customized for each program as needed.
- A list of assurance deficiencies may be derived using these worksheets for a particular program.
- Other available data, as well as focused supplemental verification, may be applied to complete DO-178B objectives.
- Other alternate methods of compliance such as reengineering may also be applied to supplement objective evidence.
- FAA expects all of the objectives to be fulfilled regardless of what mix of methods are used to show compliance.

## Follow-On Activities

- FAA Consulting is now engaged in a short validation effort on the Service History Handbook (more on this in a moment).
- The Worksheets are being considered for use by the US Air Force to evaluate some legacy systems as part of the Global Air Traffic Management (GATM) effort.
- FAA Consulting has received positive feedback from two commercial companies on the usefulness of the Handbook.
- We are seeking additional feedback on the Handbook's contents. It is possible that the validation effort and any feedback from users may lead to a revision of the Handbook in the future.



## Wide Area Augmentation System (WAAS) Service History Effort

- Current research task is to examine available problem reporting and system reliability data allow for a viable service history argument
- Acceptability for certification credit is dependent on:
  - Configuration Management of the Software
  - Effectiveness of Problem Reporting
  - Stability and Maturity of Software
  - Relevance of Product Service History Environment
  - Actual Error Rates
  - Impact of Modifications

Does not apply to WAAS since the environment is not changing

## WAAS PSH Effort Cont'd

- Effort involves:
  - Identification of all available, relevant data
  - Evaluation of that data using the Handbook
  - Identification of any gaps which might prevent a service history argument
  - Formulation of a suggested means of filling the gaps in data collection going forward
  - Creation of a service history argument or reasons why such an argument can not be created in accordance with DO-178B
- Effort is expected to conclude in 3rd Quarter of 2002



## Conclusion

- Copies of the Report and Handbook may be downloaded from the FAA Software website:

  **http://av-info.faa.gov/software**

- Questions or feedback on either the Report or Handbook may be directed to Leanna Rierson or to FAA Consulting:

  **tom@faaconsulting.com** - OR -
  **uma@faaconsulting.com**

- Questions?